1Password

Balancing act

Security and productivity in the age of AI

1PASSWORD STATE OF ENTERPRISE SECURITY REPORT 2024

Table of contents

Executive summary

Today's organizations face a no-win situation, with two crucial concerns – security and productivity – increasingly at odds. The longstanding tension between these competing priorities has taken on new urgency in a landscape constantly remade by mounting cyberthreats and disruptive technologies like AI.

To understand how organizations across industries are balancing the need to protect themselves against the pressure to deliver results, 1Password surveyed 1,500 North American white-collar employees – including 500 IT security professionals.

Leaders shouldn't have to choose between productivity and security. But our findings reveal that many feel forced to do just that. Increasingly stretched between two mission-critical imperatives, half of security professionals say it's nearly impossible to strike the right balance.

If organizations could ever afford to be lax on security, they certainly can't now. The average financial impact of cybersecurity events has grown 15% over the past three years, to a staggering $4.45 million, according to IBM's latest Cost of a Data Breach report.

At the same time, employees are under increasing pressure to perform. To boost efficiency, they're embracing disruptive technologies like AI, unapproved applications, remote work, and personal (rather than work-issued) devices.

Security professionals can't keep up. This leaves organizations struggling to protect themselves against unauthorized apps and solutions, accessed from a broad range of devices, across unsecured networks at coffee shops, hotels, airports, and homes around the world.

Well-intentioned employees and bad actors alike are experimenting with tools and techniques unique to our age of technological disruption. Today's organizations need new ways to harmonize the productivity and security that are essential to their success.

Key findings

SECURITY ON EDGE

An impossible balance

Half of security pros (50%) say it's almost impossible to find the right balance between security and employee productivity.

Experts agree: Security isn't up to snuff

79% of security pros don't feel their security protections are adequate.

Enter the AI era

92% of security pros have security concerns about generative AI. Among their top worries: employees entering sensitive company data into an AI tool (48%), using AI systems trained with incorrect or malicious data (44%), or falling for AI-enhanced phishing attempts (42%).

Top threats

More than a third of security pros list external threats like phishing or ransomware (36%), internal threats like shadow IT (36%), and/or human error (35%) among the top three threats to their organizations.

BREACH-BOOSTING BEHAVIORS

Perpetual password failure

61% of employees have poor password practices, like reusing passwords or neglecting to reset the IT-selected defaults. Workers at the level of manager or above are especially likely to have password practices that increase their organization's vulnerability to breaches.

Sprawling shadow IT

One in three employees (34%) use unapproved apps and tools, otherwise known as shadow IT. On average, these workers use a total of five shadow IT apps or tools – each representing a potential new threat vector.

It's not business – it's personal

Nearly one in five employees (17%) admit to never working on their work-provided devices, opting solely for personal or public computers.

Lax on security

More than half of employees (54%) admit to being lax about their company's security policies. Reasons include a desire to get things done quickly and be productive (24%) and the belief that security policies are inconvenient (11%) or too stringent and unreasonable (11%).

SEARCHING FOR SOLUTIONS

Security spread thin

More than two-thirds of security pros (69%) admit they're at least partly reactive when it comes to security. The main reason: They're being pulled in too many conflicting directions (61%).

A desire for complete solutions

One in three security teams (32%) have switched security tools or vendors in the past year to ones that provide more complete end-to-end solutions.

Split incentives

Fewer than one in 10 security pros (9%) say that employee convenience is their top consideration when selecting security software. But nearly half of employees (44%) are motivated by convenience.

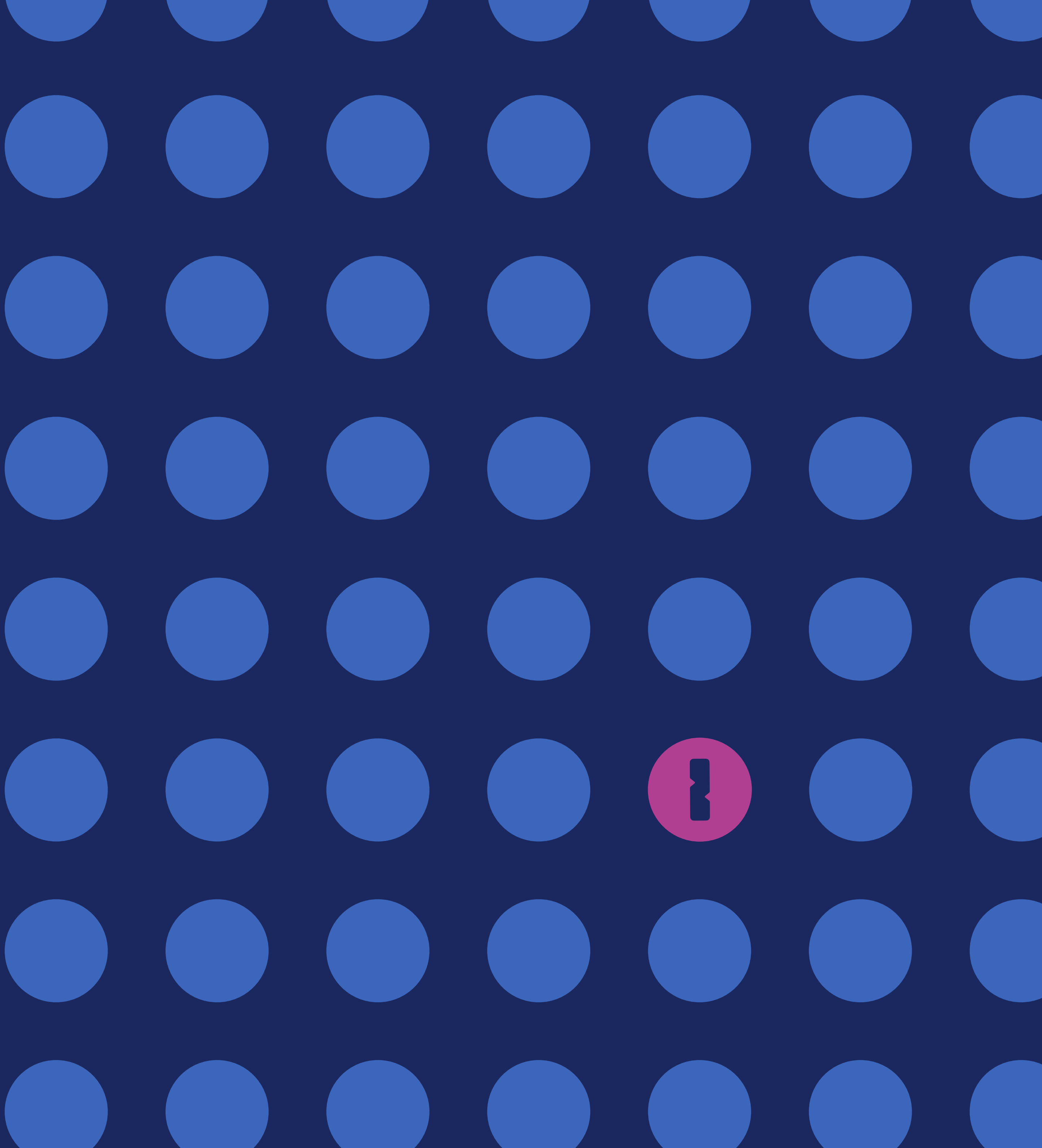
SSO is not enough

More than two-thirds of security pros (69%) say single sign-on (SSO) tools are not a complete solution for securing employees' identity.

01

Security struggles

IT teams are working hard to expand employees’ access to new tools and technologies – including AI. But they’re also increasingly concerned about security threats and feel unequipped to keep their organizations safe.



A race with no finish line

Technology is evolving so quickly that security teams can't keep up, despite admirable efforts to safeguard their organizations while allowing employees to access a broader portfolio of tech tools.

GIVING EMPLOYEES WHAT THEY WANT

80%

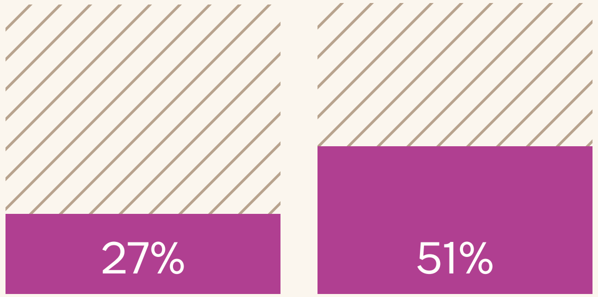
of organizations maintained or expanded the volume of apps and tools available to employees in 2023.

TEETERING ON THE EDGE

50%

of security pros say it's almost impossible to find the right balance between security and employee productivity.

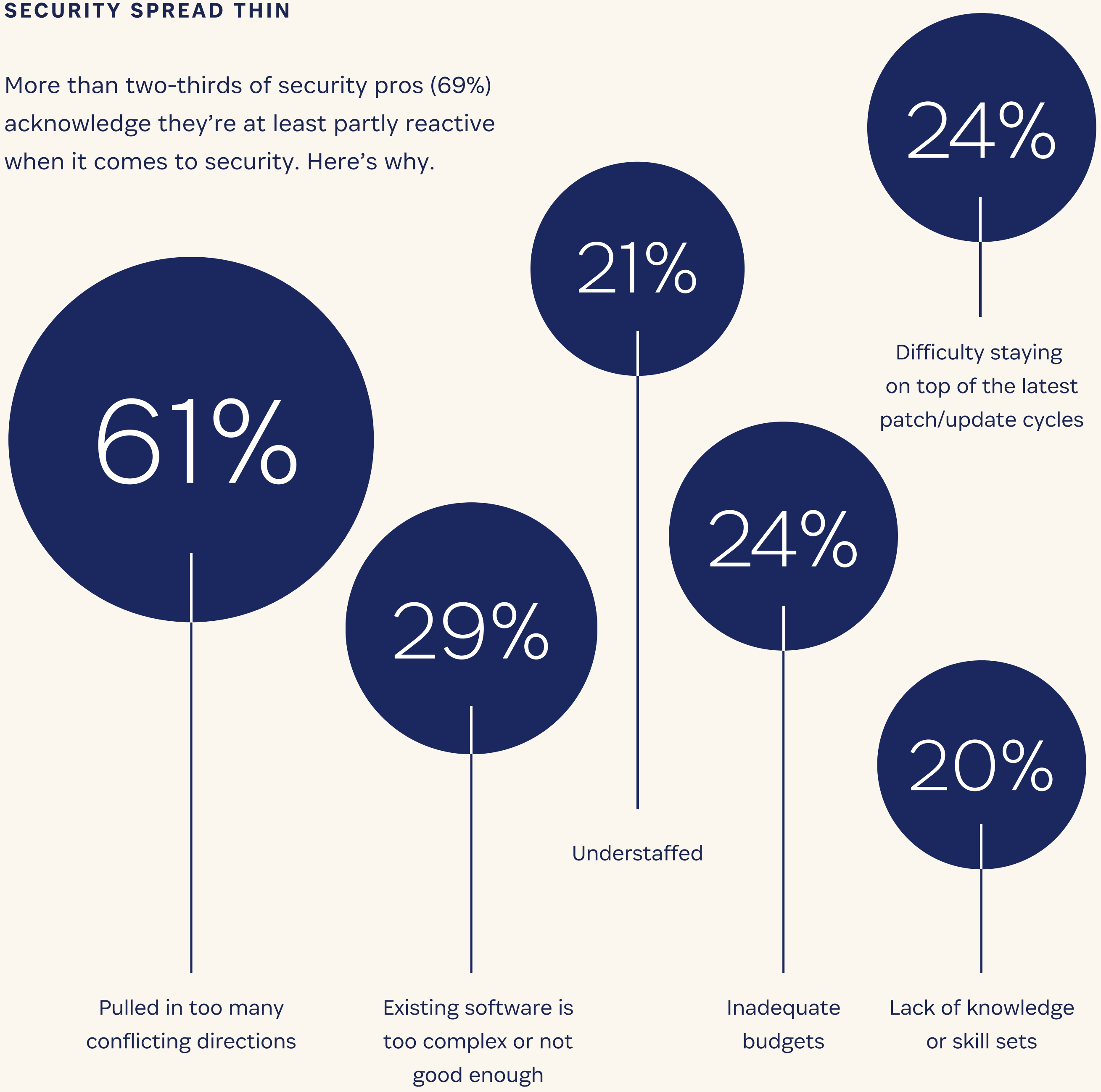
NEW TECH, NEW CHALLENGES



One in four security pros (27%) say that emerging, unproven technologies (like AI) are some of the biggest security threats their company faces today. And half of security pros (51%) say their company is struggling to safeguard employees as they use these new technologies.

SECURITY SPREAD THIN

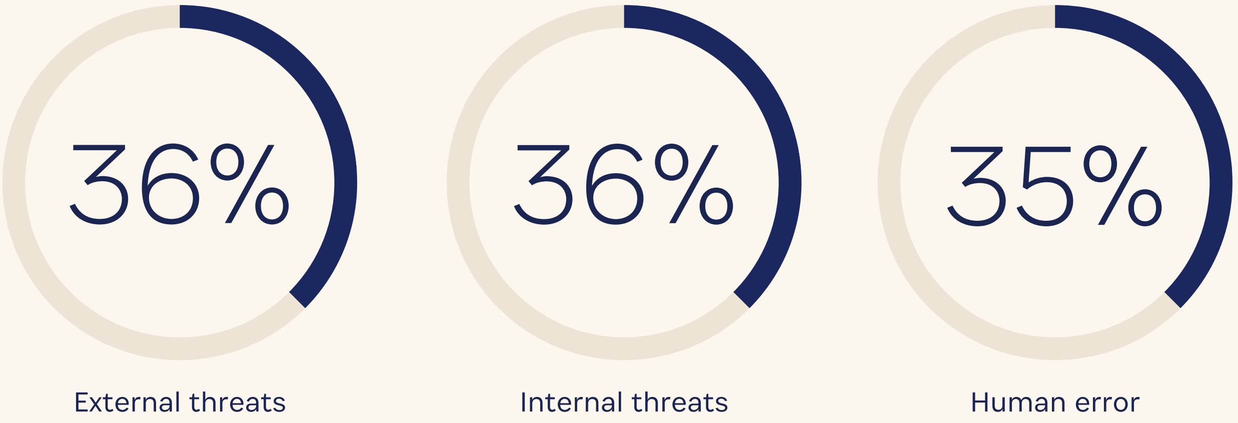
More than two-thirds of security pros (69%) acknowledge they're at least partly reactive when it comes to security. Here's why.



Threats from all directions

We asked security pros what keeps them up at night. Their responses reveal that they’re worried about threats coming from all directions.

IT ON EDGE



Asked what they see as the top threats to their organizations, 36% of security pros cited external threats like phishing or ransomware among the top three risks; 36% cited internal threats like shadow IT; and 35% cited human error.

DANGEROUSLY VULNERABLE

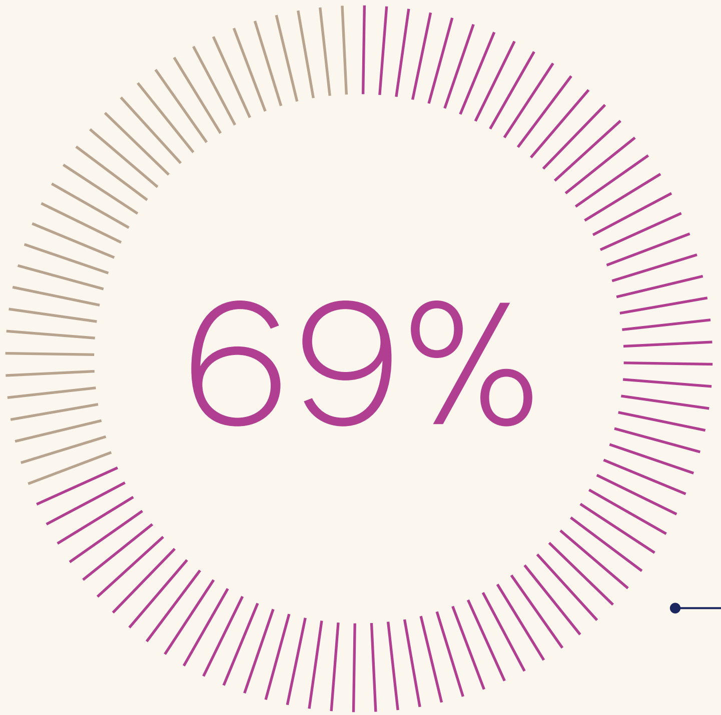
Four in five security pros (79%) don’t feel their security protections are adequate.

INCOMPLETE SOLUTIONS

30%

Fewer than one in three security pros are extremely confident that their current tooling provides a complete security solution.

SSO ISN’T ENOUGH



More than two in three security pros say single sign-on tools are not a complete solution for securing employees’ identity.

THREATS FROM ALL DIRECTIONS:

Sleepless nights

Here’s what security pros say keeps them awake in the wee hours.

“Employees not following policy and accessing restricted sites or using their personal devices.”

“An employee falling for a phishing scam.”

“The challenges of preventing AI from becoming a security risk.”

“Trying to keep up with all the new software and the way that they're getting into our software.”

“Not knowing if remote users are using good practices when working in their homes.”

“The rapid pace at which security threats arise, as well as their ever-evolving complexity and intelligence.”

“Knowing it only takes one incident.”

“We have sensitive data – but an aging workforce that doesn’t want to learn new things.”

02

For employees, productivity is paramount

Employees are under intense pressure to perform. They gravitate toward tools, technologies, devices, and habits that make it easy to be productive – often without considering the impact on security.

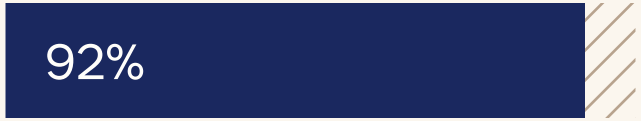
Shadow IT and the need to be productive

Employees seize on whatever apps and tools help them deliver results – regardless of whether they're employer-approved.

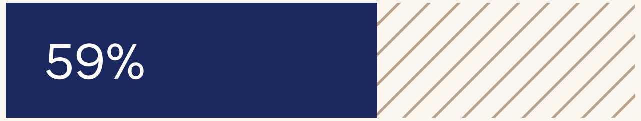
APP CREEP

Employees who rely on shadow IT use an average of five unapproved apps or tools – each representing a potential new threat vector.

POLICIES EXIST, BUT ENFORCEMENT'S A MISS



92% of security pros say their company policy requires IT approval to download and use software and apps for work.



But 59% of security pros say they don't control whether employees follow these policies – potentially because they lack enforcement capabilities.

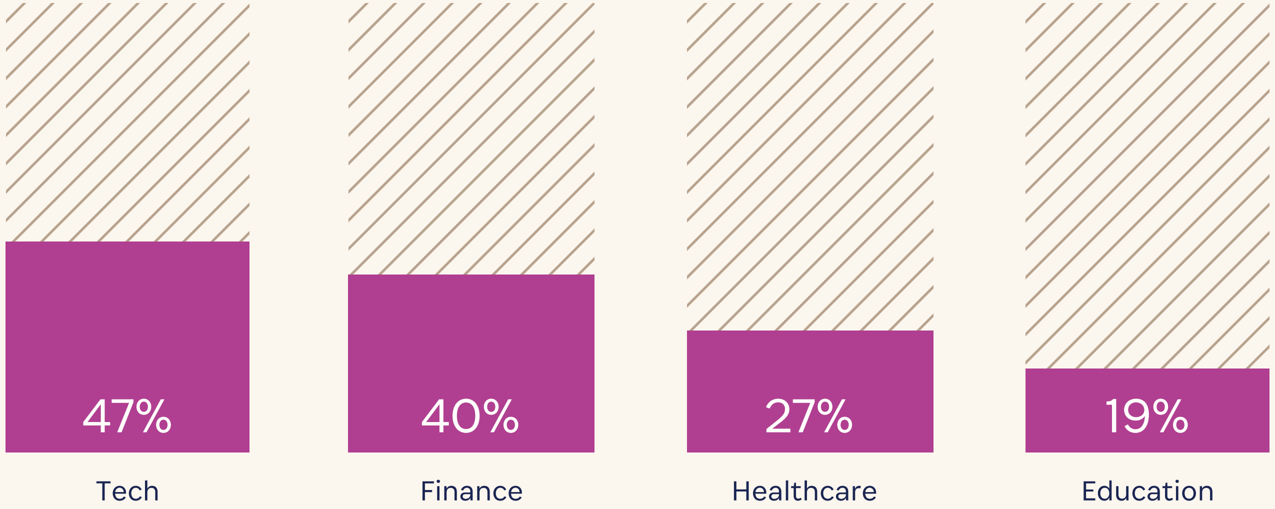
DISRUPTING THE BALANCE

64% of security pros say shadow IT makes navigating employee convenience and security challenging.

STICKY SHADOW IT

34% Despite years of employee education and the deployment of security management software, one in three workers use unapproved apps or tools – otherwise known as shadow IT.

TECH-SECTOR PRODUCTIVITY PRESSURE



Nearly half of tech industry employees (47%) use shadow IT apps or tools, compared to 40% of employees in finance, 27% in healthcare, and 19% in education. Of those who rely on shadow IT, tech industry employees use an average of six shadow IT apps/tools, compared to four in finance, four in education, and three in healthcare.

Blurred lines between personal and work devices

As employees embrace remote and hybrid work and use their personal devices for professional purposes, it's getting harder for security pros to monitor the universe they're charged with protecting.

OUT OF SIGHT

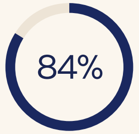
65%

Nearly two in three security pros say that personal devices have made complete visibility into employee security habits much more elusive.

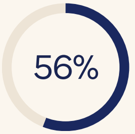
ALL TOO PERSONAL

17%

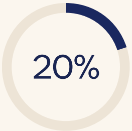
of employees admit to never working on their work-provided devices – opting solely for personal or public computers.



More than four in five security pros say their company asks that employees only use work-provided devices.



More than half of employees have worked on a personal device in the last year.



One in five employees have worked on public computers or from a friend's or family member's device.

Security? Not my job.

Security may be keeping IT teams up all night – but employees' minds are elsewhere.

SPEEDING PAST SECURITY

54%

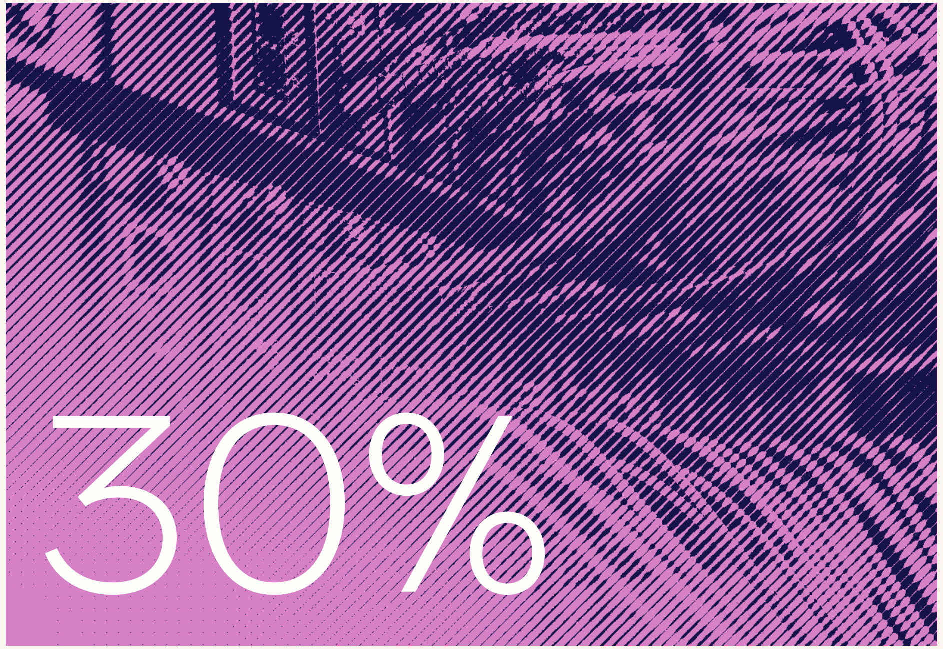
More than half of employees admit to being lax on their company's security policies. Here's why.

24%
say they're just trying to get things done quickly and be productive.

11%
say security policies are inconvenient.

11%
say security policies are too stringent or unreasonable.

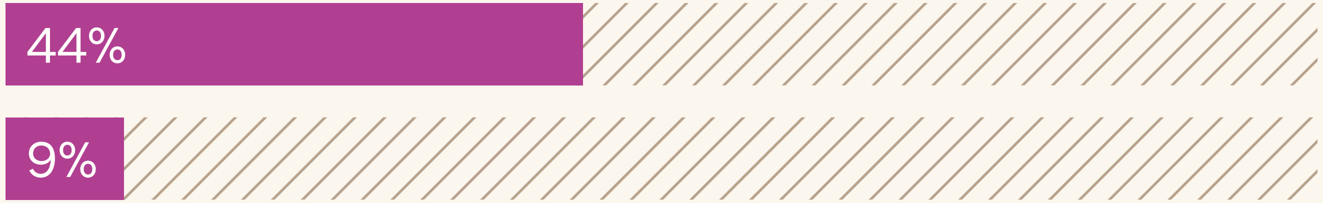
LEAVE IT TO IT



30%

Nearly one in three employees say that security is for the IT team to deal with – and that it's not their job.

SECURITY VS. CONVENIENCE



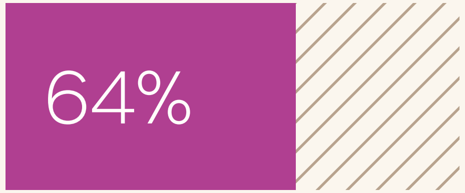
Nearly half of employees (44%) say security would be less of an issue if leaders made tools easier to use and policies easier to follow.

But fewer than one in 10 security pros (9%) say that employee convenience is the top consideration driving their security software decisions.

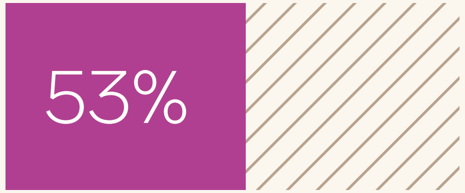
Bad habits, big risks

In the race for productivity, many employees take security shortcuts that can put their organizations at risk.

DO AS I SAY



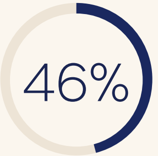
of managers and higher admit to poor password practices…



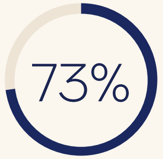
compared to 53% of lower-level employees.

SKIPPING SOFTWARE UPDATES

Software updates and patches can be pivotal to preventing breaches. But updates on a laptop can be time consuming and interrupt the workday. Meanwhile, many IT pros recommend delaying updates to avoid the bugs common to new software. Employees are understandably confused.



Fewer than half of employees update software immediately upon receiving an alert to do so.



Three-quarters say they're too busy or don't want to interrupt their work.

PASSWORD PROBLEMS

23%

say most of their passwords follow a similar pattern or are identical.

19%

say they have the same passwords across multiple work accounts.

14%

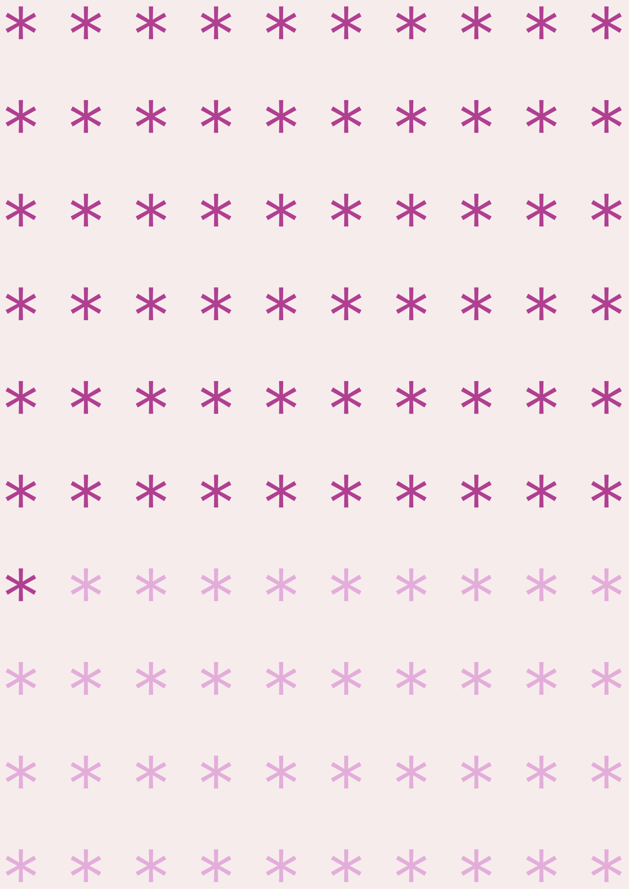
say their passwords are IT-selected defaults that they've never changed.

13%

text or email passwords between work and home devices.

61%

of employees have poor password practices.

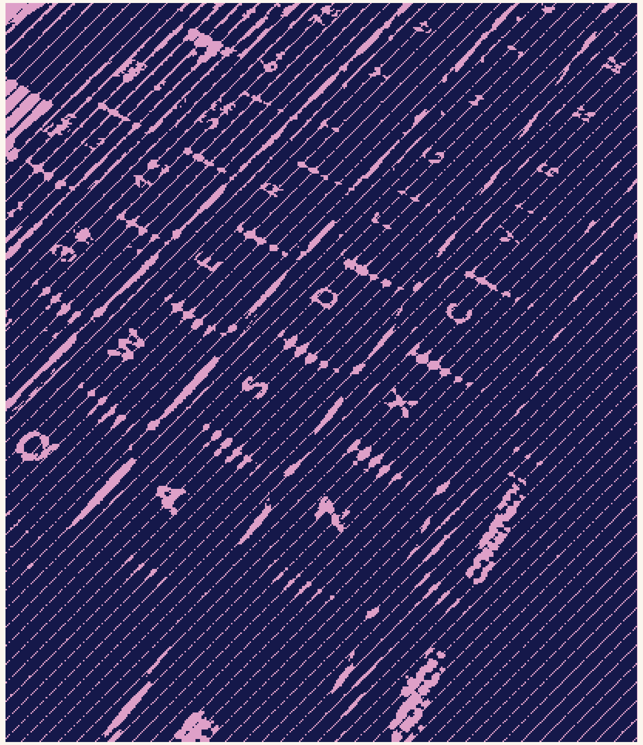


> Knowing it only takes one incident.
>
> — IT Security Director, software company

Security slips

Employees know that security threats are pervasive. Even so, security slip-ups are all too common – increasing organizations' vulnerability.

PHANTOM FRIENDS

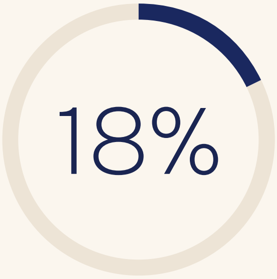


61%

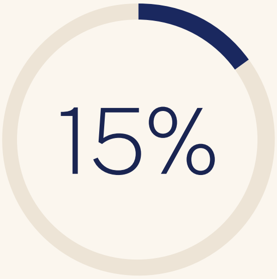
of employees have been – or have seen a colleague be – the target of a phishing attack from someone posing as a CEO, manager, colleague, vendor, client, or other work associate.

A YEAR OF SLIP-UPS

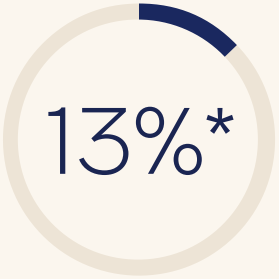
Half of employees (50%) acknowledge they've made security slip-ups in the past year.



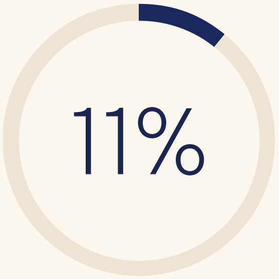
clicked a link in a suspicious email.



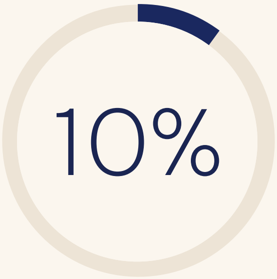
logged in to a work account from a personal device against company policy.



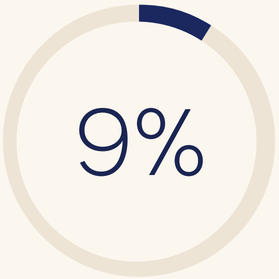
maintained access to company tools or resources after leaving the organization.



went against IT policy to get work done more efficiently.



worked in company documents from a personal account in a violation of company policy.



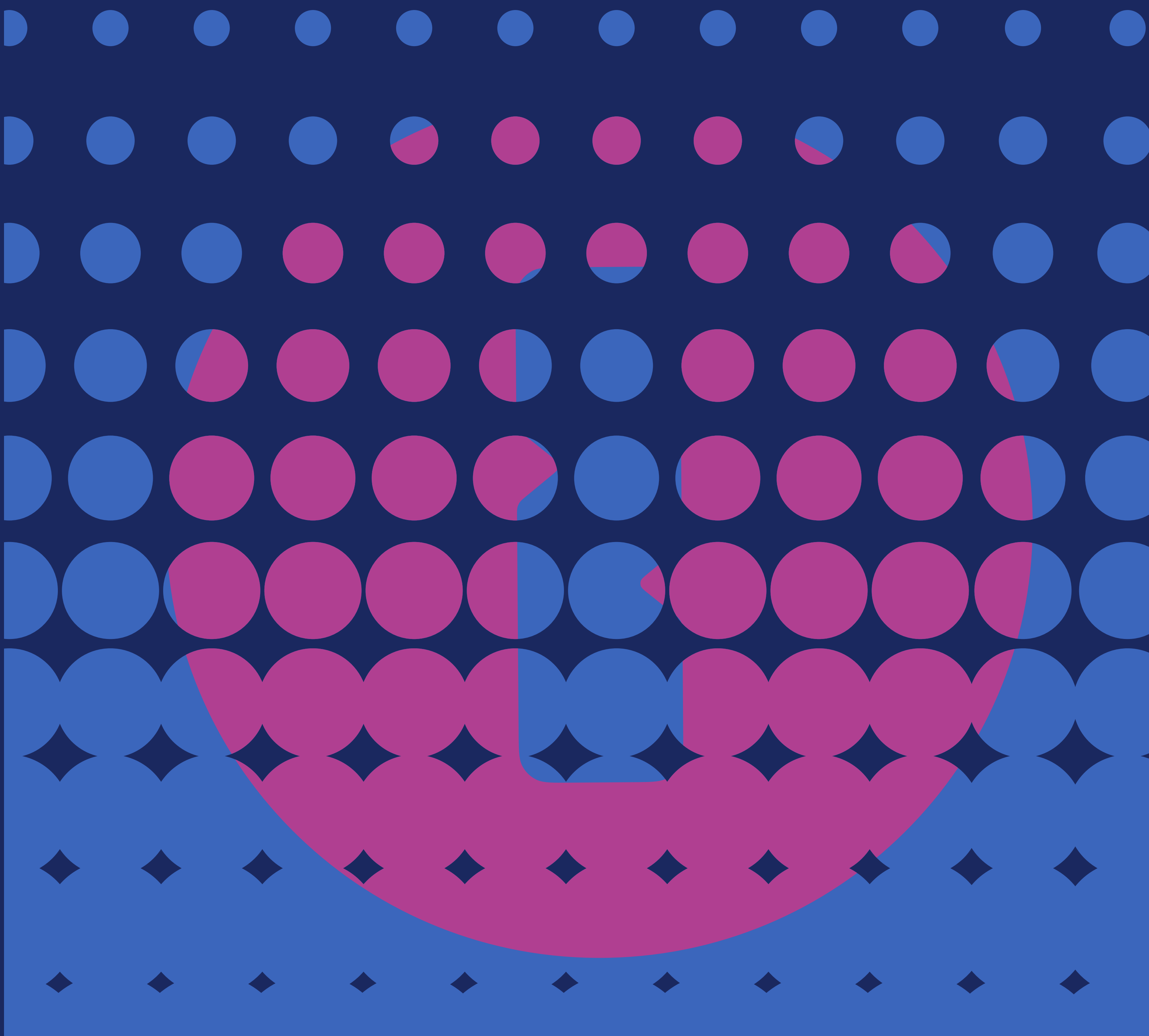
shared credentials for work tools with people outside the company.

* This finding highlights a weakness in employee offboarding processes that could have devastating consequences.

03

Enter generative AI

The rise of generative AI has accelerated the tug-of-war between those who prioritize security and those who emphasize productivity. While security teams are worried about generative AI's impact on breaches and vulnerabilities, employees are excited about its potential to make them more productive and efficient.



Generative AI: productivity dream, security nightmare

Security teams are working hard to create and enforce new policies around this rapidly evolving technology.

NEW RESOURCES FOR A NEW THREAT

Nearly two in three security teams (61%) increased their focus on AI in 2023.

40%

of teams implemented new AI-specific security tools.

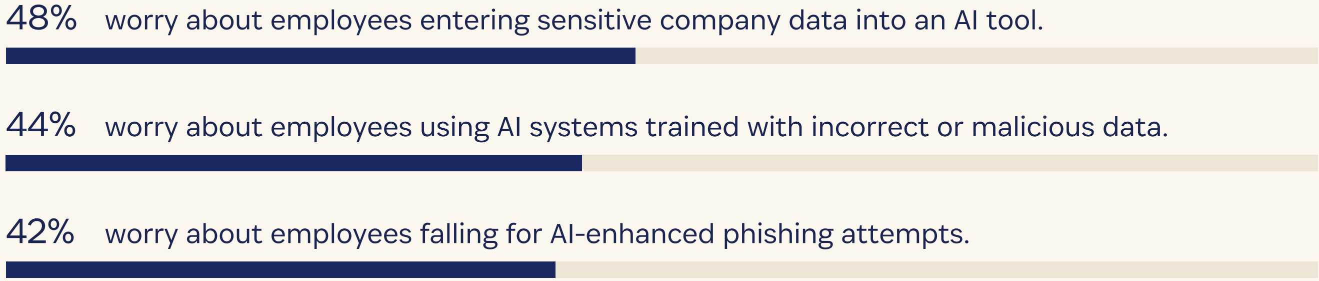
42%

of teams hired IT or security workers with AI-specific expertise.

OVERWHELMING CONCERN

92%

of security pros have security concerns around AI.



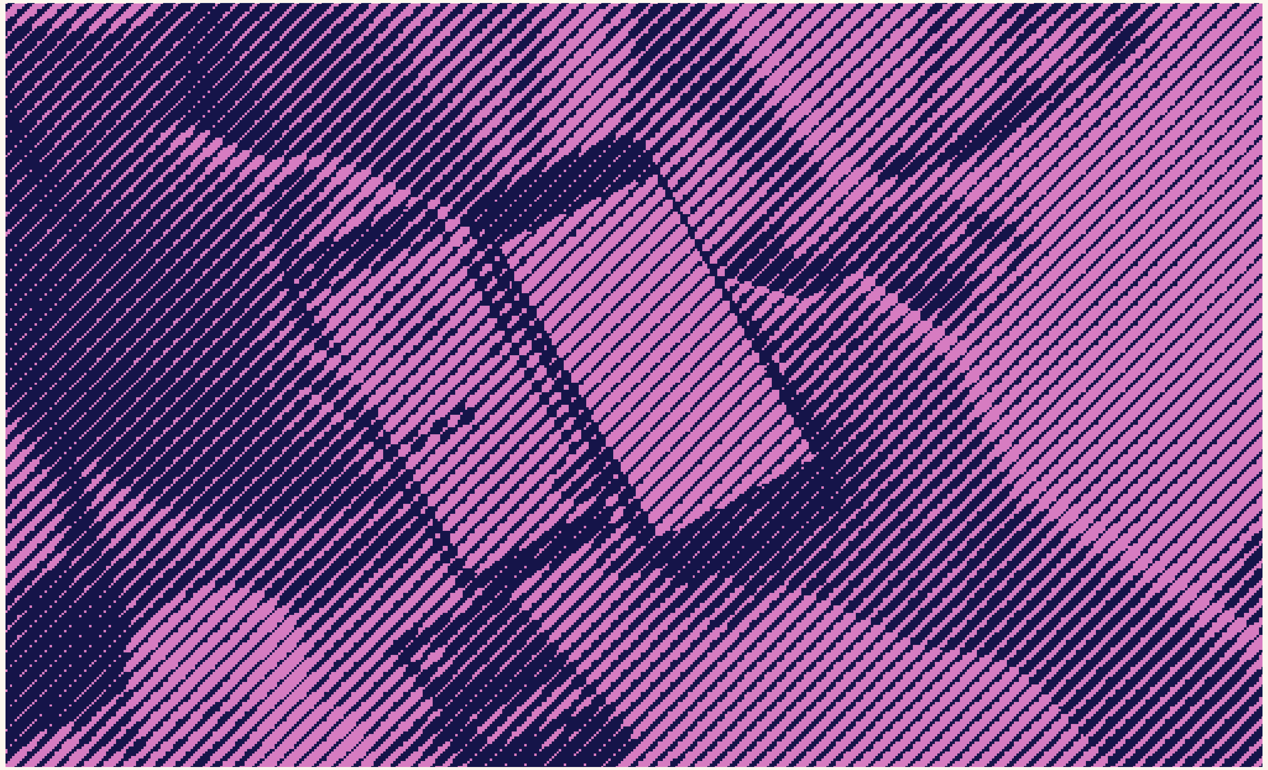
48% worry about employees entering sensitive company data into an AI tool.

44% worry about employees using AI systems trained with incorrect or malicious data.

42% worry about employees falling for AI-enhanced phishing attempts.

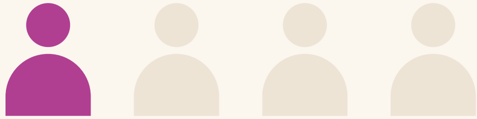
Risks? What risks?

Employees are enticed by generative AI's promise to boost efficiency. And when it comes to security, they don't see what the fuss is all about.



AI RENEGADES

A relatively small, but significant, group of employees knowingly violate company rules on the use of generative AI.

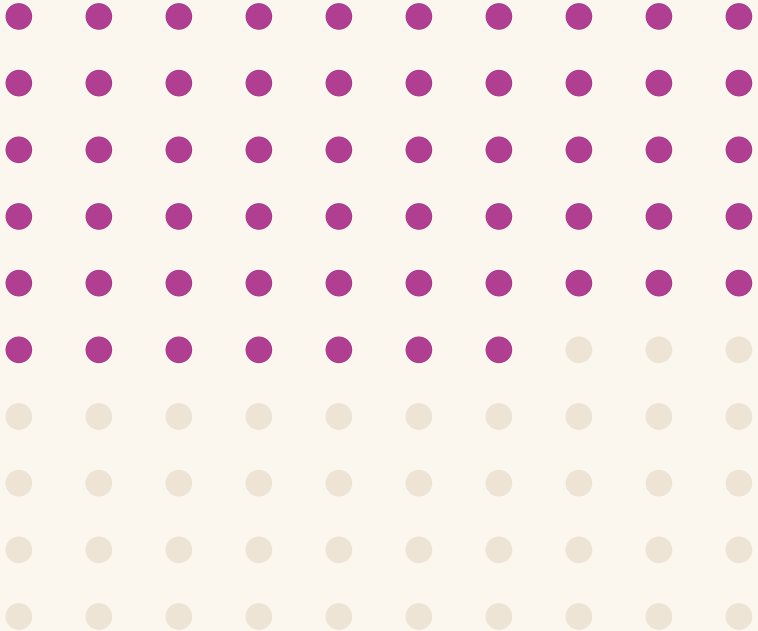


One in four employees (26%) don't understand the security concerns over using AI tools at work.

22%

One in five employees admit to not always following their company's AI policies.

RETURN ON AI



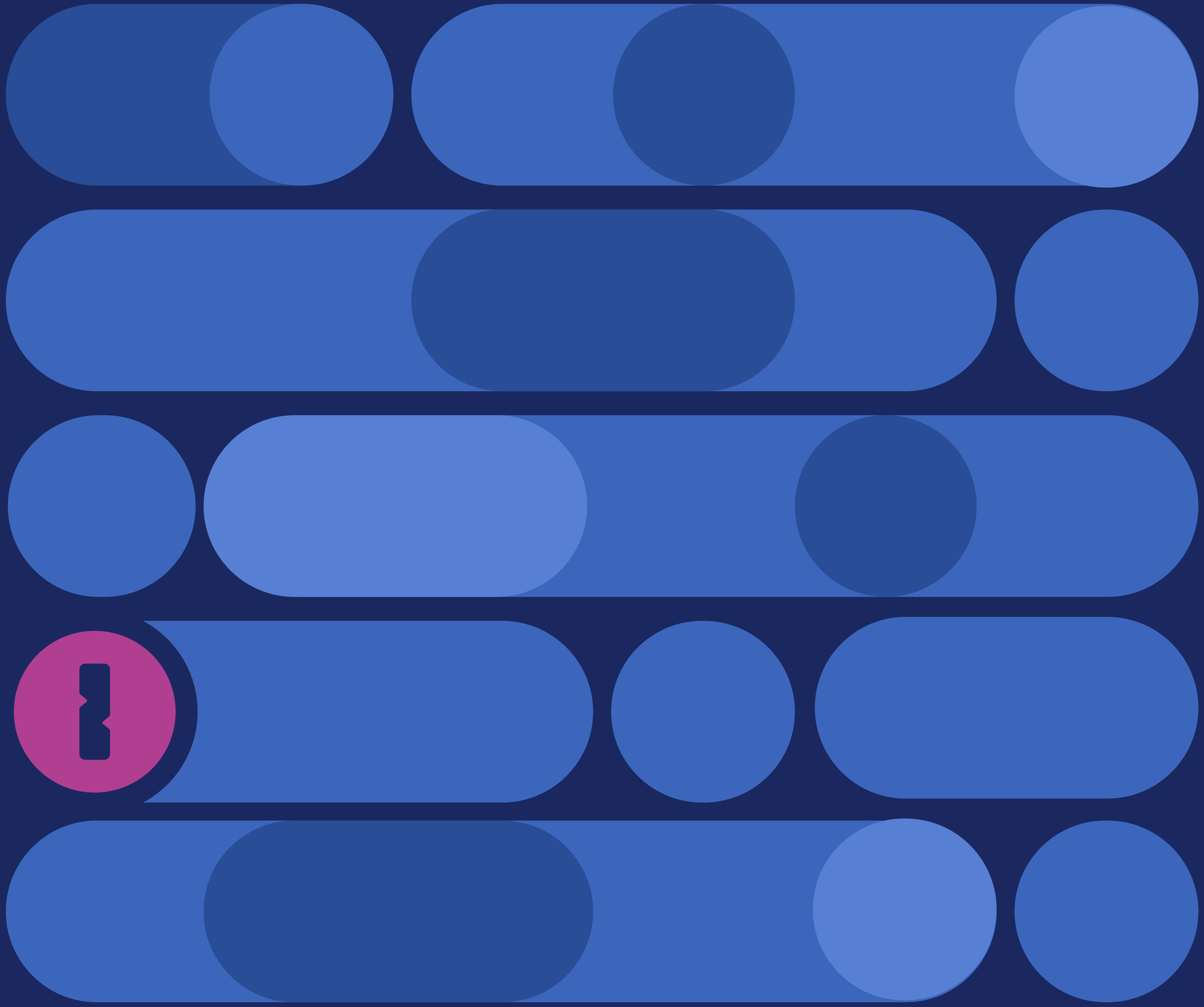
57%

More than half of employees say that using generative AI tools at work saves them time and makes them more productive.

04

Security solution shuffle

Today's employees often bring software suggestions to their companies, instead of the other way around. To be responsive to employees while minimizing threats, security teams are reshuffling their solution stacks. Amid increasing complexity, it's harder than ever to deploy a comprehensive solution that keeps employees happy and companies secure.

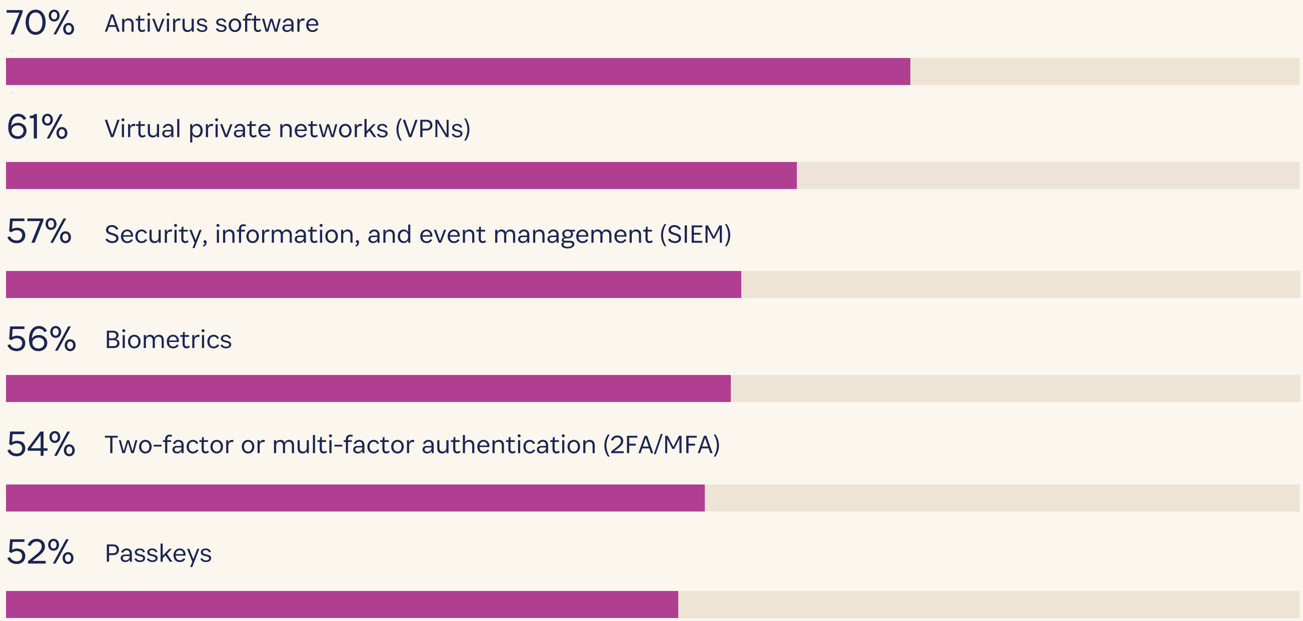


An imperfect patchwork

Security teams are cobbling together multiple tools to accommodate employees' requests while addressing threats coming from all directions. But they don't feel they have complete trust in any of these combinations – and continue to seek comprehensive solutions.

A GROWING SECURITY STACK

Here are some of the most common technologies companies are using to secure employees.



SECURITY SWITCH-UP

One in three security teams (32%) have switched security tools or vendors in the past year to ones that provide more complete end-to-end solutions.

> "Phishing scams, ransomware attacks, and a patchwork system give our security team heartburn. They're the tireless ninjas keeping the bad guys out, so next time you see them, offer a coffee (or a medal). We're in this digital battle together."
>
> — IT Security VP, tech hardware company

REMOTE WORK SECURITY

To protect employees working remotely, 61% of security pros limit work access on unapproved hardware.

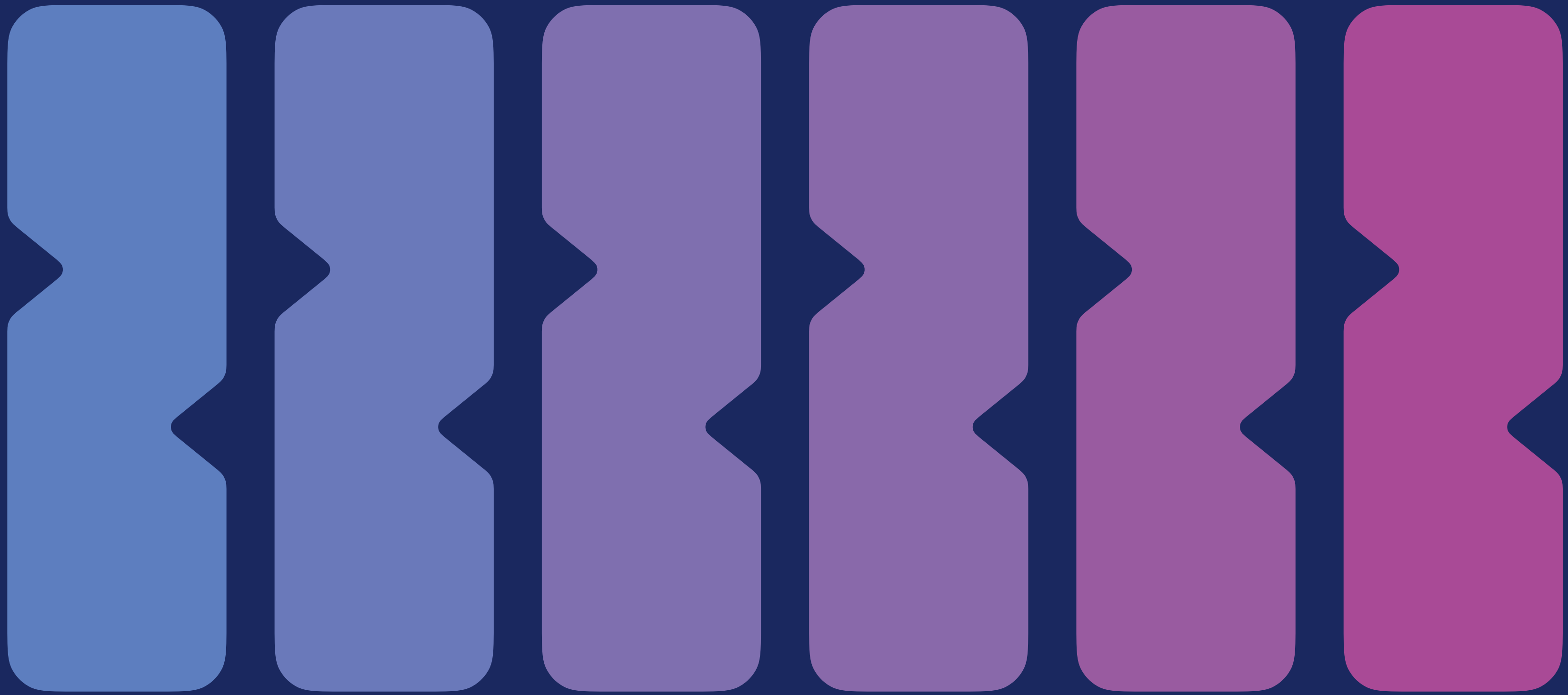
50%

require employees to turn on 2FA/MFA for all apps.

49%

require the use of a VPN to access company data.

1Password



05

Conclusion

Businesses shouldn’t have to balance the security of their data, assets, and reputations against the efficiency and convenience that their people expect. In a rapidly shifting landscape, where new cyberthreats and disruptive technologies are constantly emerging, organizations deserve solutions that harmonize security and productivity.

Moving forward, it will be incumbent upon businesses and security providers to deliver solutions that magnify human brilliance while maximizing organizational security – regardless of what threats and opportunities lie ahead.

“Employees have unprecedented flexibility in where and how they work, which often extends to the apps and devices they use. This creates significant security challenges for IT and security leaders, who often feel like they don’t have bandwidth or budget to safeguard their organizations. When it comes to security and productivity, it shouldn’t be either-or. It’s time for businesses and security providers to deliver solutions that keep employees protected and productive – no matter how or where they prefer to work. When you secure your people, you secure your business.”

— Jeff Shiner, CEO, 1Password

1Password conducted this research using an online survey prepared by Method Research and distributed by PureSpectrum among n=1,500 adults (age 18+) in the United States and Canada who are full-time employees in white-collar positions, including a subset of n=500 IT security professionals. The sample included minimum quotas (n=300+) for manager and higher titles, and was balanced across company size.
Data was collected from January 2 to January 11, 2024.

1Password's annual report, which showcases data from 1,500 North American IT security professionals and white-collar employees, explores pressing top security challenges faced by businesses, with a focus on the tension between productivity and security. The study found that today's CISOs and security leaders face more challenges than ever, including the implications of ever-evolving tech and the escalating threat landscape, while employees' top concern remains working flexibly and efficiently. Between securing against shadow IT and safely rolling out new technologies like AI, IT teams are facing an almost impossible balance between security and productivity.

1Password